Sentinel

Vigenère

The first cipher with a key

DEFENDING OUR DIGITAL WAY OF LIFE

Recap

Using these numbers, we can represent all the different letters!

Character	Code	Binary
A	65	1000001
B	66	1000010
a	97	1100001
0	30	11110

This is called the **ASCII character encoding**

Recap

Strings have the charCodeAt method:

```
"A".charCodeAt(0)
// 65
```

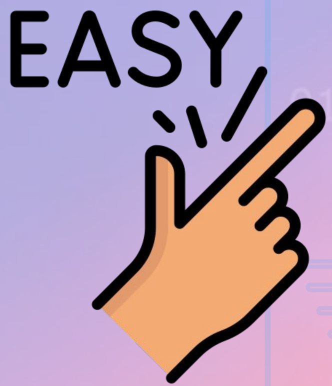
ASCII code for “A”: 65

And to convert a code to a string:

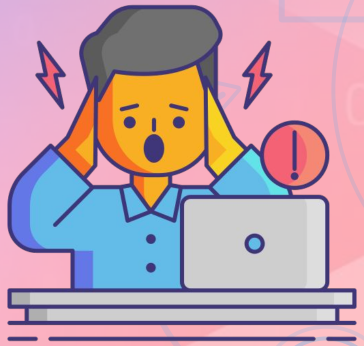
```
String.fromCharCode(65)
```

The problem

Cryptanalysis of Caesar and Mixed Alphabet Ciphers is too easy…



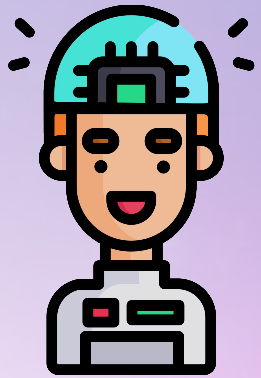
A bit of frequency analysis and bam! The encryption is broken!



Breaking the Pattern

How can we break the underlying patterns that allow frequency analysis?

What if we switch between different substitution ciphers mid-cipher?



E.g. encrypt each letter with Caesar with a different shift

Caesar++

"BREAKING THE PATTERN"

Plaintext	Shift	Ciphertext
B	1	C
R	2	T
E	3	H
A	4	E
K	5	P
I	6	O
N	7	U
G	8	O

Both I and G are encrypted to be O!

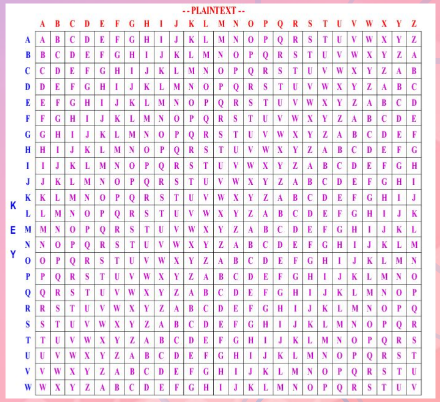
The underlying language frequencies are lost 😈

Polyalphabetic Ciphers

Substitution Ciphers that use multiple substitution alphabets

The most famous is called the Vigenère cipher

It took almost **300 years** to break it!!!😱



-- PLAINTEXT --

KEY

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

Vigenère

Choose a key, any key

Repeat the key so it’s as long as the ciphertext

Plaintext: BREAK ME IF YOU CAN
Key: TOAST
Repeat: TOASTTOASTTOAST

Vigenère

Use each letter of the key as a Caesar shift!

So A = 0, B = 1, C = 2, … Z = 25

For each letter: ciphertext = (plaintext + key) % 26

So in effect we have a series of interwoven Caesar Ciphers!

Encrypt Example

“BREAK ME IF YOU CAN”

Key: “TOAST”

B	R	E	A	K	M	E
T	O	A	S	T	T	O
U	F	E	S	D	F	S

(B + T) % 26
= 1 + 19
= U

(R + O) % 26
= (17 + 14) % 26
= 5 = F

(M + T) % 26
= (12 + 19) % 26
= F

Decrypt Example

“BREAK ME IF YOU CAN”

Key: “TOAST”

U	F	E	S	D	F	S
T	O	A	S	T	T	O
B	R	E	A	K	M	E

(U - T) % 26
= 2
= B

(F - O) % 26
= (5 - 14) % 26
= -9 % 26

Negative results should “wrap around” from the end of the alphabet:
(-9 + 26) % 26 = 17 = R

Coding Vigenère

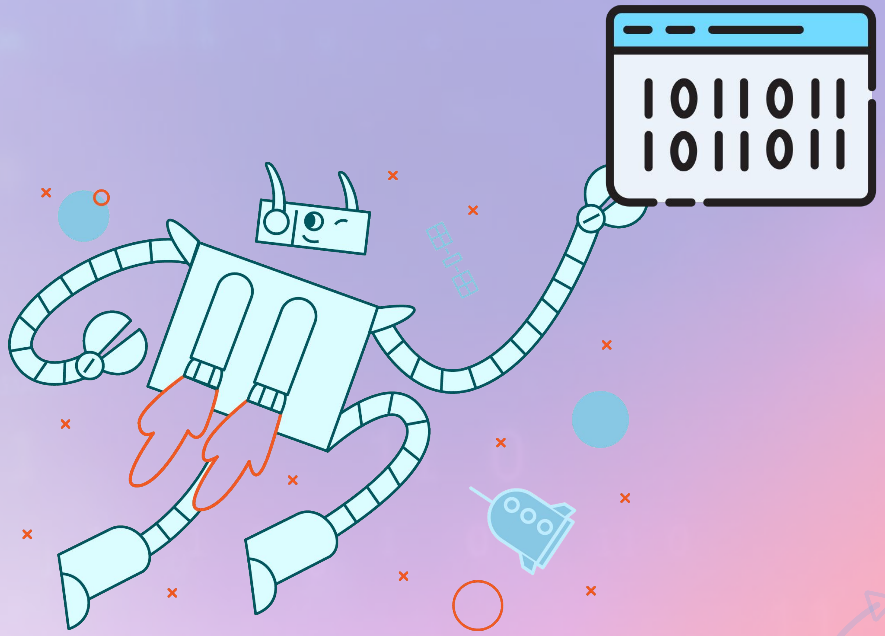
In order to write a Vigenère encryptor, we'll have to talk about how computers represent letters

You all have heard that computers only understand 1s and 0s: Binary

But using Binary they are able to represent numbers

Binary

1	1
2	10
3	11
4	100
…	…



We won't dive into binary encoding of numbers just yet

Vigenère in JS

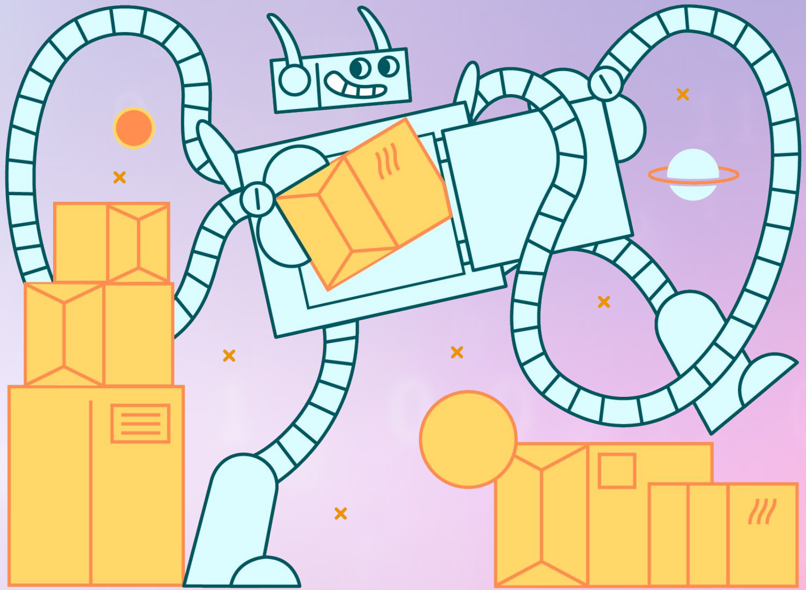
In Vigenère A = 0, B = 1, ... Z = 25

How can we convert a character in JS to it’s alphabetic position?

```
"S".charCodeAt(0) - 65
// 18
```

Let’s encrypt!

Now you have all the knowledge and tools to implement your own Vigenère encryptor and decryptor!



Let’s encrypt!

1 Write the encryptor and decryptor

2 Encrypt a message

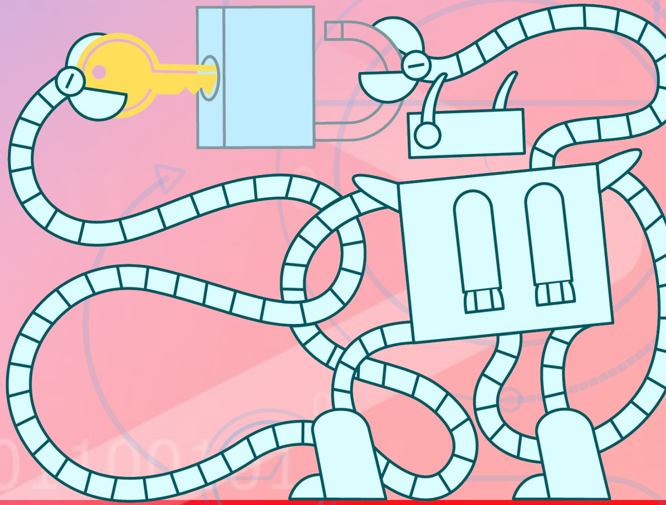
3 Secretly share the key with a friend

4 See if they can decrypt your message using their decryptor and the key

Breaking Vigenère

Simple frequency analysis won't work…

But, if we're able to find the length of the key, we can break each Caesar Cipher individually!



Finding The Key Length

Plaintext: THE FOX AND THE CAT

Key: LOL

Ciphertext: EVP QCI LBO EVP NOE

We can see patterns in the ciphertext of length 3

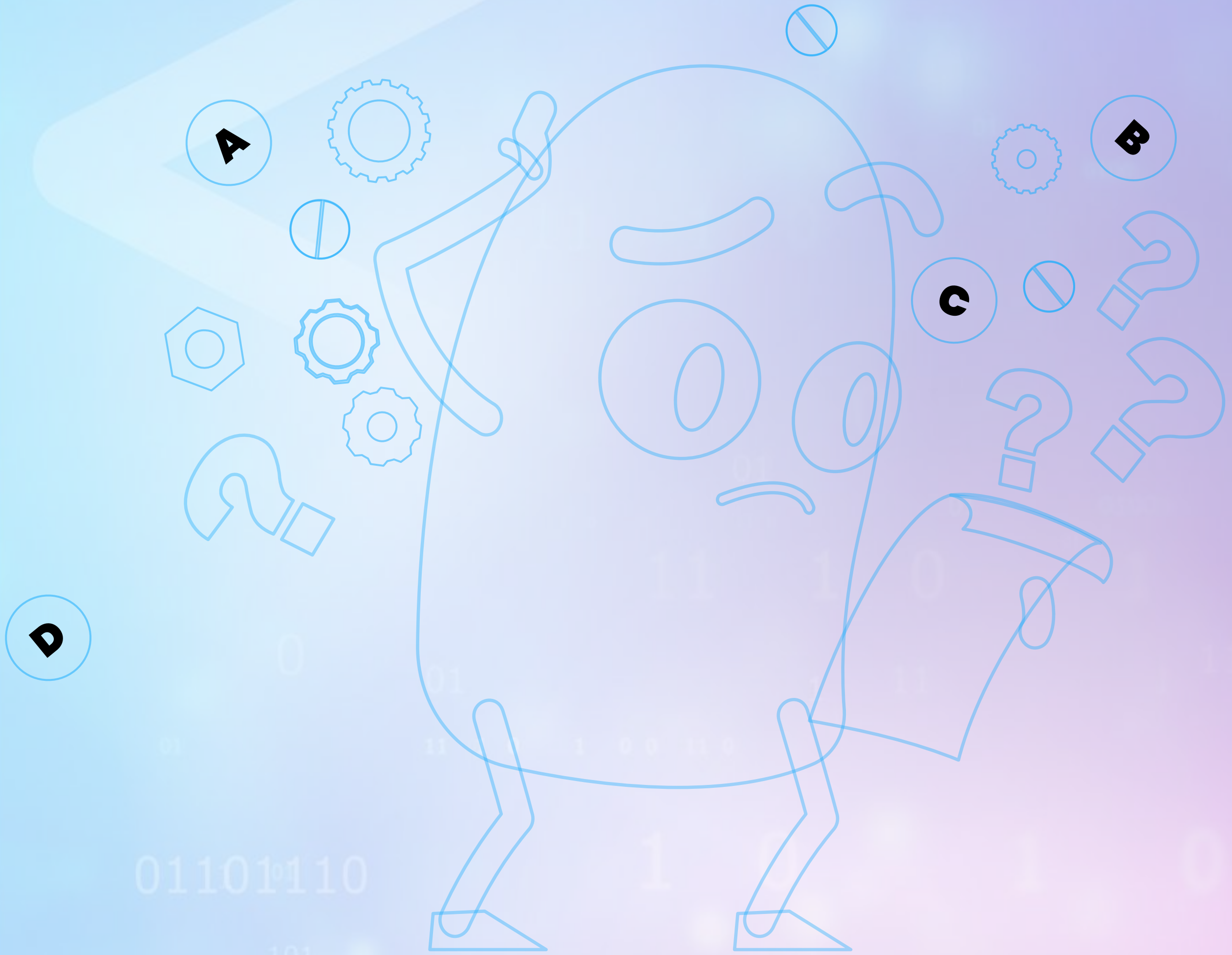
Breaking the Code

Now we just need to break 3 Caesar Ciphers:
EVP QCI LBO **EVP** NOE

1	**2**	**3**
E	V	P
Q	C	I
L	B	O
E	V	P
N	O	E

How?

- Brute Force
- Frequency Analysis



Questions?

Sentinel

Your Turn!

> Play around, have fun, ask questions!